Elliptic Curves with Supersingular Reduction over Γ-extensions

A.G. Nasybullin

1

Let p be a prime number, k_0 a finite extension of the rationals $\mathbb{Q}$, k_∞/k_0 a Galois extension with [Galois] group Γ isomorphic to the group of p-adic integers $\mathbb{Z}_p$. Put $\Gamma_n := \Gamma^{p^n}, k_n := k_\infty^{\Gamma_n}$. Let E be an elliptic curve over $\mathbb{Q}$ with supersingular reduction at p, $E(k_n)$ the k_n-rational points of E, and $Ш_n^{(p)}$ the p-component of the Shafarevich-Tate group of the curve $E \otimes k_n$.

Theorem 1.1. *We assume the following conditions:*

(a) p is not 2 and does not divide the number of the rational connected components of bad reduction of the curve $E \otimes k_0$.

(b) For all places v of k_0 dividing p, the completion $k_{0,v}$ is unramified over the field of the p-adic numbers $\mathbb{Q}_p$, and its degree over $\mathbb{Q}_p$ is not divisible by 4.

(c) The Γ-extension k_∞/k_0 is cyclotomic, i.e.

$$k_\infty \subset \bigcup_{n=1}^{\infty} k_0(\sqrt[p^n]{1})$$

Then, if $E(k_0)$ is finite and $Ш_0^{(p)} = 0$, the groups $E(k_n), E(k_\infty)$ and $Ш_n^{(p)}$ are finite and

$$\log_p[Ш_n^{(p)}] = [k_0 : \mathbb{Q}] \left(\left[\frac{p^{n+1}}{p^2-1} \right] - \left[\frac{n+1}{2} \right] \right).$$

We denote by a_p the trace of the Frobenius automorphism of the reduction of $E \mod p$. Note that $E \mod p$ is supersingular if and only if it is non-singular and p divides a_p. Consequently, $a_p = 0$ for $p > 3$ and $a_p = 0, \pm p$ when $p = 2, 3$.

Theorem 1.2. *Suppose that $k_0/\mathbb{Q}$ is abelian and k_∞/k_0 is cyclotomic. Then:*

(a) There are integers $\rho^{(0)}, \rho^{(1)} \geq 0$, equal for $a_p \neq 0$, such that for all sufficiently large $n \equiv s \mod 2$ $(s = 0, 1)$,

$$\operatorname{rk} E(k_n) + \operatorname{cork} Ш_n^{(p)} - \operatorname{rk} E(k_{n-1}) - \operatorname{cork} Ш_{n-1}^{(p)} = \rho^{(s)}(p^n - p^{n-1}),$$

where $\operatorname{rk} E(k_n)$ is the rank of $E(k_n)$ and $\operatorname{cork} Ш_n^{(p)}$ is the corank of $Ш_n^{(p)}$;

(b) if $a_p \neq 0$ and the degree $[k_0 : \mathbb{Q}]$ divides a number of the form $(p^l + 1)p^m$, then $\operatorname{rk} E(k_n)$ stabilizes, and consequently $E(k_\infty)$ is finitely generated;

(c) if $E(k_0)$ and $Ш_0^{(p)}$ are finite, and for $a_p = 0$ we have the condition (b) of Theorem 1.1, then $\rho^{(0)} = \rho^{(1)} = 0$, i.e. $\operatorname{rk} E(k_n)$ and $\operatorname{cork} Ш_n^{(p)}$ stabilize;

(d) if $\rho^{(0)} = \rho^{(1)} = 0$, then there are integers $\mu^{(s)}, \delta^{(s)} \geq 0, \lambda^{(s)} (s = 0, 1)$ such that $\delta^{(0)} = \delta^{(1)} = 0$ for $a_p = 0$ and for all sufficiently large $n \equiv s \mod 2$,

$$\log_p[Ш_n^{(p)}] - \log_p[Ш_{n-1}^{(p)}] = \mu^{(s)}(p^n - p^{n-1}) + ([k_0 : \mathbb{Q}] - \delta^{(s)}) \left[\frac{p^n}{p+1} \right] + \delta^{(s)} \left[\frac{p^{n-1}}{p+1} \right] + \lambda^{(s)},$$

where $Ш_n^{(p)}$ is the cotorsion of $Ш_n^{(p)}$.

Denote by T_n the set of places of the field k_n dividing p and ramified in k_∞.

Theorem 1.3. *Suppose that $a_p = 0$ and that for all n and $v \in T_n$, the extensions $k_{n,v}/\mathbb{Q}_p$ are abelian. Then there are integers $\rho^{(s)}, r^{(s)}, \nu^{(s)}, \mu^{(s)}, \lambda^{(s)}$ $(s = 0, 1)$, μ_i $(i = 1, 2, \cdots)$, satisfying the relations*

$$\rho^{(s)} \geq r^{(s)} \geq \nu^{(s)} \geq 0, \qquad \rho^{(0)} - r^{(0)} = \rho^{(1)} - r^{(1)},$$

$$\mu_1 \geq \mu_2 \geq \cdots \geq 0, \mu_i = 0 \text{ for } i > \min(\nu^{(0)}, \nu^{(1)}),$$

$$\mu^{(s)} \geq 0,\ r^{(0)} + r^{(1)} \leq r, \text{ where } r = \sum_{v \in T_0} [k_{0,v} : \mathbb{Q}_p] \leq [k_0 : \mathbb{Q}],$$

and such that for sufficiently large $n \equiv s \mod 2$ the following assertions hold:

(a) $\operatorname{rk} E(k_n) + \operatorname{cork} Ш_n^{(p)} - \operatorname{rk} E(k_{n-1}) - \operatorname{cork} Ш_{n-1}^{(p)} = \rho^{(s)}(p^n - p^{n-1})$;

(b) $\log_p[Ш_n^{(p)}] - \log_p[Ш_{n-1}^{(p)}] =$

$$\mu^{(s)}(p^n - p^{n-1}) + (r - r^{(s)} + \nu^{(s)}) \left[\frac{p^n}{p+1}\right] - \sum_{i=1}^{\nu^{(s)}} \left[\frac{p^{n-\mu_i}}{p+1}\right] - \sum_{i=1}^{r^{(1-s)}} \left[\frac{p^{n-\mu_i}}{p+1}\right] + \lambda^{(s)};$$

(c) if $r^{(s)} = 0$, then $\operatorname{rk} E(k_n) = rk E(k_{n-1})$;

(d) if $\operatorname{cork} Ш_n^{(p)}$ stabilizes, then $\operatorname{rk} B_n - \operatorname{rk} B_{n-1} = r^{(s)}(p^n - p^{n-1})$, where B_n is the image of $E(k_n) \otimes \mathbb{Z}_p \to \sum_{v \in T_n} E(k_{n,v})^{(p)}$ and $\operatorname{rk} B_n$ is the rank of B_n over $\mathbb{Z}_p$.

In the case of nonsupersingular reduction, the behavior of the groups $E(k_n)$ and $Ш_n^{(p)}$ has been investigated by B. Mazur (see [1], [2]). One of the main points of his research is the description of the Γ-modules $E(k_{n,v})^{(p)}$ for $v \in T_n$. Analogously, the proofs of Theorems 1.1, 1.2, and 1.3 are based on the theorem in the following paragraph.

2 The Local Group of Points

Let E be an elliptic curve over $\mathbb{Q}_p$, $E \mod p$ be supersingular, a_p the trace of the Frobenius automorphism on the reduction $E \mod p$. For any abelian extension $K/\mathbb{Q}_p$, set $K_n := K \cap \mathbb{Q}_p^{nr}(\zeta_n)$, where $n = -1, 0, 1, \cdots; \mathbb{Q}_p^{nr}$ denotes the maximal unramified extension of $\mathbb{Q}_p$, and ζ_n a primitive root of unity of degree p^{n+1} if $p \neq 2$, and of degree p^{n+2} if $p = 2$. We will denote by $m(K)$ the smallest n for which $K_n = K$.

Theorem 2.1. *Let $K/\mathbb{Q}_p$ be a finite abelian extension with [Galois] group $G = \operatorname{Gal}(K/\mathbb{Q}_p)$. Then the $\mathbb{Z}_p[G]$-module $E(K)^{(p)}$ is free of p-torsion and has a system of generators $\{e_n | n = -1, -, \cdots, m(K)\}$, all of whose relations can be derived from the following:*

$$e_n \in E(K_n),$$

$$\operatorname{Nor}_{n/n-1} e_n = a_p e_{n-1} - e_{n-2} \qquad (n \geq 2),$$

$$\operatorname{Nor}_{1/0} e_1 = \begin{cases} a_p e_0 - [K_0(\zeta_0) : K_0] e_{-1}, & (p \neq 2), \\ a_p e_0 - [K_0(\zeta_0) : K_0](a_p - F - F^{-1}) e_{-1}, & (p = 2), \end{cases}$$

$$\operatorname{Nor}_{0/-1} e_0 = \begin{cases} (a_p - F - F^{-1}) e_{-1}, & (p \neq 2), \\ (a_p^2 - a_p F - a_p F^{-1} - 1) e_{-1}, & (p = 2), \end{cases}$$

where $\operatorname{Nor}_{n/n-1} : E(K_n) \to E(K_{n-1})$ is the norm homomorphism and $F \in \operatorname{Gal}(K_{-1}/\mathbb{Q}_p)$ is the Frobenius automorphism.

The author would like to thank Yu. I. Manin for posing the problem and his constant interest in working on it, and V. G. Berkovich for helpful discussions. *(translated by Igor Minevich and Florian Sprung.)*

References

[1] Yu. Manin: *Cyclotomic Fields and Modular Curves*, Uspehi Matematičeskih Nauk **26:6** (1971), 7-71.

[2] B. Mazur: *Rational Points of Abelian Varieties with Values in Towers of Number Fields*, Inventiones Mathematicae[1] **18** (1972), 183-266.

Received 20 October 1976

[1]The original article referenced the translation into Russian, found in
Matematika: Periodicheskiĭ sbornik perevodov inostrannykh stateĭ. Tom 17 (1973), vyp. 3. (Russian) [Mathematics: Periodical collection of translations of foreign articles. Vol. 17 (1973), no. 3] Izdat. "Mir", Moscow, 1973. 157 pp.